REMARKS

As a preliminary matter, Applicants wish to thank the Examiner for thorough examination of the present application as evidenced in the Office Action dated April 27, 2009. The present Amendment and Response is responsive to the Office Action dated April 27, 2009. Claims 1-4 and 8-16 remain pending. No new matter has been added. Claims have been amended as described below in the section entitled "Claim rejections under 35 USC §112".

Claim Rejections under 35 USC §112

Claims 1-4 and 8-16 stand rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The applicant respectfully argues the rejected claims after amendments conform to the provisions of 35 USC §112.

As per claim 1:

It is indicated in this office action, "claim 1 recites the limitation a signatory (S) selecting a braid x generated from the left subgroup $L B_m (l)$, a second braid x' generated from the braid group $B_n (l)$, and a third braid a generated from the braid group $B_n (l)$, by computer, wherein the computer is adapted to making them meet $x'=a^{-1}xa$, moreover, with known x and x', it being **impossible** to find a in calculation, and considering the braid pair(x',x) as a public key of signatory (S), the braid a as a private key of signatory (S); however, there is no further explanation in the specification how with known x and x' , it being **impossible** to find a in calculation, and considering the braid pair(x',x) as a public key of signatory (S), the braid a as a private key of signatory (S)" (emphasis added).

The applicant submits, in paragraph [0061] of publication specification, the present invention discloses: "The called CSP problem means: for a given conjugacy pair(x,y) $\in B_n \times B_n (x \sim y)$, finding a braid $a \in B_n$, which makes $y=a^{-1}xa$. For braid group, there is no efficient arithmetic which can solve the CSP problem in multinomial time currently, therefore, for a conjugacy pair(x,y) $\in B_n \times B_n$ selected randomly, their CSP problem will be a difficult problem with high probability".

That is to say, so far the CSP problem (conjugacy search problem)—"with known x and x', it being **impossible** to find a in calculation" (emphasis added)—has been a difficult problem in the art of algorithmic number theory and has not been solved by an efficient arithmetic that is widely-known by people of ordinary skill in the art. Thus, no further explanation of "with known *x* and *x'*, it being **impossible** to find *a* in calculation" is required in the claims. The description in claim 1, "with known *x* and *x'*, it being **impossible** to find a in calculation", merely aims to emphasize a prerequisite to the application of the present invention.

Furthermore, the CSP problem exactly makes the signature method with high confidentiality, which has been the technique basis for the present invention: the security of the signature method proposed in the present invention is established on the difficulty of the MCSP problem (matching conjugacy search problem), which is proved to have a same difficulty with CSP problem. Thus, in claim 1 of present invention, the braid pair (*x',x*) may be considered as a public key of signatory (*S)* and the braid *a* as a private key of signatory (*S)*. In other words, with the known public key, it is impossible to find the private key in calculation, which ensures that the signature method of the present invention maintains high confidentiality.

Therefore, claim 1 is definite for particularly pointing out and distinctly claiming the subject matter which applicant regards as the invention, which conforms to 35 USC §112. Accordingly, reconsideration and withdrawal of the subject matter rejection of this claim are requested.

As per claims 2-4 and 13-14:

As stated above, independent claim 1 complies with the requirements of 35 USC §112. Thus, for at least the reasons noted above in regard to independent claim 1, applicants respectfully submit that dependent claims 2-4 and 13-14, which ultimately depend from independent claim 1, are also in conformity with the provisions of 35 USC §112. Accordingly, reconsideration and withdrawal of the subject matter rejection of these claims are requested.

As per claim 8:

Claim 8 is another method implementation based on the method claimed in claim 1 and comprises all the elements of claim 1. For at least the reasons noted above in regard to independent claim 1, claim 8 is definite for particularly pointing out and distinctly claiming the subject matter which applicant regards as the invention, which conforms to 35 USC §112. Accordingly, reconsideration and withdrawal of the subject matter rejection of this claim are requested.

As per claims 9-12 and 15-16:

As stated above, independent claim 8 complies with the requirements of 35 USC §112. Thus, for at least the reasons noted above in regard to claim 8, applicants respectfully submit that dependent claims 9-12 and 15-16, which ultimately depend from independent claim 8, are also in conformity with the provisions of 35 USC §112. Accordingly, reconsideration and withdrawal of the subject matter rejection of these claims are requested.

Therefore, claims 1-4 and 8-16 of the present invention conform to 35 USC §112.

Conclusion

Applicants believe that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application; the undersigned can be reached at the telephone number set out below.

The Commissioner is hereby authorized to charge any additional fees due or credit any overpayment to Deposit Account No. 50-2421.

Sincerely,

Dated: July 24, 2009

___/David R. Stevens/____
David R. Stevens
Reg. No. 38,626

Stevens Law Group
1754 Technology Drive, Suite 226
San Jose, CA 95110
Phone (408) 288-7588
Fax (408) 288-7542